

Registers of Scotland

RoS Board

September 2021

Key risk register (KRR)

Purpose

1. The purpose of this paper is to provide RoS Board with an update on the KRR following the EMT, RoS Board and Audit & Risk Committee (ARC) annual risk workshop in May 2021 and ongoing Key Risk Owner (KRO) and ARC reviews.
2. The paper supports the board in fulfilling its role to provide strategic advice to the Keeper for its focus on setting a framework of prudent and effective controls that enables risk to be assessed and managed.
3. The paper introduces a 'reporting by exception' approach to enable the board to fulfil its role as effectively and efficiently as possible.

Recommendation

4. RoS Board is requested to consider the 'reporting by exception' approach taken in this paper and advise the Keeper on its efficacy (in supporting the board fulfil its role at paragraph 2).
5. RoS Board is requested to review the KRR summary at Annex 1, the People & Change risk assessment at Annex 2 and the Cyber Resilience risk assessment at Annex 3 and advise the Keeper on the update.

Background

6. RoS KRR contains the key risk scenarios that may affect delivery of our corporate plan objectives and the risk response strategies for these threats and opportunities. The KRR is a 'live' document which is reviewed and updated at least monthly by KROs and submitted to EMT for approval as part of their monthly corporate governance review process. The KRR is also submitted to RoS Board and ARC meetings for noting and/or advice as a summary report or as the RoS Assurance Framework report.

Key risk register (KRR) reporting format

7. The paper introduces a 'reporting by exception' approach, comprising 3 elements:

Reporting element	Frequency of reporting	Board input / 'Ask' of the Board
1. RoS Key Risk profile	Every Board meeting	Advice on whether strategic risk exposure continues to be captured by KRR 2021-26
2. New/developing risks	As relevant	Advice on how risks have been assessed in terms of 'causes - risk scenario - impacts' and the risk response (i.e. controls)
3. Risks trending away from target risk score* / controls not delivering anticipated risk response	As relevant	Advice on how risks have been assessed in terms of 'causes - risk scenario - impacts' and the risk response (i.e. controls)

Key risk register – reporting element 1

8. KROs have updated the KRR at their Corporate Governance meeting monthly reviews with progressive update of risk descriptions, appetite, proximity, scoring, controls and assurance opinions. A summary of the KRR as at the date of this paper is at Annex 1. The [‘Live’](#) KRR will be available to RoS Board at its September 2021 meeting.

9. EMT April 2021 approved the following timeline of activity to complete an approval of the KRR and Assurance Framework 2021-26:

- a. EMT CG review the work in progress KRR on 27 May, 25 June and 29 July 2021 including an interim update of assurance opinions to ARC on 20 August 2021.
- b. ARC review interim RoS Assurance Framework 2021-26 on 20 August. ARC to make recommendations to the RoS Board 14/15 September.
- c. RoS Board review the KRR and ARC recommendations on the Assurance Framework 2021-26 for approval at 14/15 September 2021 meeting.

Key risk register – reporting element 2

10. The annual risk workshop concluded the “People and Change” opportunity risk in KRR 2020-25 should be re-framed as a threat risk in KRR 2021-26. Annex 2 contains the risk “bow tie” version of the re-framed threat risk.

11. The risk scenario, key risk owner, risk appetite, risk scoring, causes, impacts and controls have been identified/assessed and noted in Annex 2.

12. The KRO has assessed current control effectiveness/maturity, represented by status indicators in Annex 2 (with accompanying assessment rationale). ERM will support the KRO and control owners in identifying when and how each control (if not currently effective/mature) will develop from its current status (potentially involving a number of development steps). Effective/mature controls will be monitored and reviewed to ensure continuing effectiveness.

13. Aggregation of this data will provide a high level ‘route to target’ and enable reporting by exception (if relevant) as part of reporting element 3 at future Board meetings.

Key risk register – reporting element 3

14. The Cyber Resilience key risk has been re-assessed resulting in an increase in the likelihood assessment from Medium (3) to High (4). The overall assessment increases from 12 to 16 (remaining a ‘High’ risk response priority).

15. The re-assessment was prompted by work to respond to a recommendation in the Cyber Resilience Audit Review (Q4 2020-21). This related to improving the connection between the IT Security Risk Register and the Cyber Resilience key risk, ensuring the KRO has the necessary information to accurately assess the key risk.

16. The current assessment of this risk is now informed by the latest contents of the IT Security Risk Register, and a mechanism is being established to ensure the efficacy and robustness of the relationship between the two risk registers.

17. The increase in likelihood has been determined by risk assessments and gap analysis, providing a richer understanding of security deficiencies, the threats that could exploit them, and the approaches used by relevant threat actors to do so. To mitigate this increase, the IT Security function has a

roadmap of technical control improvements for 2021-2022 (and beyond), with the aim of reducing the likelihood of risk realisation as controls are deployed. However due to RoS's growing aspirations as a digital information business, and the constant evolution and sophistication of threat actors, their tools, and their motivations, the probability of risk realisation may continue to be High (4) until the deployed control improvements are fully mature.

18. Work continues to develop Cyber Resilience corrective controls (reducing the potential impact of this risk), with a programme of cyber resilience exercises planned for September 2021. This will provide assurance of the effectiveness of existing controls and identify improvement opportunities. The current impact assessment for this risk will be reviewed after this work to determine when and if a reduction from 'Exceptional' (4) to 'Major' (3) is justifiable.

19. Annex 3 contains the full Cyber Resilience key risk assessment. A 'route to target' graph is being developed to indicate visually when and how new/existing controls are anticipated to reduce likelihood and impact (and overall exposure to this risk). Variations in progress towards the target will be reported to the Board.

Conclusion

20. RoS Board to review the Key Risk profile at Annex 1, the People & Change risk assessment at Annex 2, the Cyber Resilience risk assessment at Annex 3 and consider the background, topic matter and recommendations in this paper for advice to the Keeper.

Head of Enterprise Risk Management
Corporate
27 August 2021

Annex 1 – KRR Summary

Threats								
1. Financial Health	Current Score 12 ▼ 3 vs Inherent ↔ 0 vs Last Month	Target Score 4	Risk Appetite Minimalist	2. Financial Capability	Current Score 12 ▼ 3 vs Inherent ↔ 0 vs Last Month	Target Score 9	Risk Appetite Cautious	
3. Operational Capacity	Current Score 15 ▼ 0 vs Inherent ▼ 1 vs Last Month	Target Score 6	Risk Appetite Cautious	4. LRC - Ministerial Target 2024	Current Score 12 ▼ 0 vs Inherent ↔ 0 vs Last Month	Target Score 4	Risk Appetite Minimalist	
5. Public Trust in the Registers	Current Score 8 ▼ 2 vs Inherent ↔ 0 vs Last Month	Target Score 4	Risk Appetite Minimalist	6. Uncertainty of future business model beyond 2024	Current Score 8 ▼ 0 vs Inherent ↔ 0 vs Last Month	Target Score 6	Risk Appetite Cautious	
7. People and Change	Current Score 25 ▼ 0 vs Inherent ↔ 0 vs Last Month	Target Score 4	Risk Appetite Minimalist	8. Cyber Resilience	Current Score 16 ▼ 9 vs Inherent ▲ 4 vs Last Month	Target Score 9	Risk Appetite Cautious	
9. Product Sustainability	Current Score 16 ▼ 4 vs Inherent ↔ 0 vs Last Month	Target Score 9	Risk Appetite Cautious				Risk Response Treat	
Opportunities								
10. LRC - Realising Benefits	Current Score 2 ▲ 1 vs Inherent ↔ 0 vs Last Month	Target Score 16	Risk Appetite Open	11. Maximising Use of RoS Data	Current Score 4 ▲ 3 vs Inherent ↔ 0 vs Last Month	Target Score 20	Risk Appetite Open	
12. Sustain and Improve Customer Experience	Current Score 12 ▲ 11 vs Inherent ↔ 0 vs Last Month	Target Score 20	Risk Appetite Open	13. Relationship with SG	Current Score 9 ▲ 8 vs Inherent ↔ 0 vs Last Month	Target Score 16	Risk Appetite Open	
							Risk Response Treat	

Risk Tolerance Thresholds for Threats and Opportunities

The combination of likelihood and impact rating provides a mechanism to prioritise risk response.

